UNITED
NATIONS

A

General Assembly

Distr.
GENERAL

A/CN.9/437
12 March 1997

ORIGINAL: ENGLISH

UNITED NATIONS COMMISSION
ON INTERNATIONAL TRADE LAW
Thirtieth session
Vienna, 12-30 May 1997

REPORT OF THE WORKING GROUP ON ELECTRONIC COMMERCE ON THE WORK OF ITS THIRTY-FIRST SESSION (New York, 18-28 February 1997)

CONTENTS

	Paragraphs	Page
INTRODUCTION	1-15	3
I. DELIBERATIONS AND DECISIONS	16	6
II. LEGAL ISSUES AND POSSIBLE PROVISIONS TO BE CONSIDERED IN UNIFORM RULES ON DIGITAL SIGNATURES	17-150	6
A. General remarks	17-24	6
B. Specific legal issues and draft provisions	25-150	9
1. Definitions	29-50	10
(a) Digital signature	30-38	10
(b) Authorized certification authorities	39-50	13
2. Liability	51-73	17
3. Issues of cross-border certification	74-89	25

	Paragraphs	Page
1. Definitions (continued)	90-113	29
(b) Authorized certification authorities (continued)	90-97	29
(c) Certificates	98-113	31
4. Signatures by legal and natural persons	114-117	36
5. Attribution of digitally-signed messages	118-124	37
6. Revocation of certificates	125-139	39
7. Register of certificates	140-148	42
8. Relations between users and certification authorities	149-150	44
III. INCORPORATION BY REFERENCE	151-155	45
IV. FUTURE WORK	156-157	46

INTRODUCTION

1. Upon adoption of the UNCITRAL Model Law on Electronic Commerce (hereinafter referred to as "the Model Law"), the Commission, at its twenty-ninth session (1996), proceeded with a discussion of future work in the field of electronic commerce, based on a preliminary debate held by the Working Group on Electronic Data Interchange at its thirtieth session (A/CN.9/421, paras. 109-119). It was generally agreed that UNCITRAL should continue its work on the preparation of legal standards that could bring predictability to electronic commerce, thereby enhancing trade in all regions.

2. New proposals were made as to possible topics and priorities for future work. One proposal was that the Commission should start preparing rules on digital signatures. It was stated that the establishment of digital signature laws, together with laws recognizing the actions of "certifying authorities" (hereinafter referred to as "certification authorities"), or other persons authorized to issue electronic certificates or other forms of assurances as to the origin and attribution of messages "signed" digitally, was regarded in many countries as essential for the development of electronic commerce. It was pointed out that the ability to rely on digital signatures would be a key to the growth of contracting as well as the transferability of rights to goods or other interests through electronic media. In a number of jurisdictions, new laws governing digital signatures were currently being prepared. It was reported that such law development was already non-uniform. Should the Commission decide to undertake work in that area, it would have an opportunity to harmonize the new laws, or at least to establish common principles in the field of electronic signatures, and thus to provide an international infrastructure for such commercial activity.

3. Considerable support was expressed in favour of the proposal. It was generally felt, however, that, should the Commission decide to undertake work in the field of digital signatures through its Working Group on Electronic Data Interchange, it should give the Working Group a precise mandate. It was also felt that, since it was impossible for UNCITRAL to embark on the preparation of technical standards, care should be taken that it would not become involved in the technical issues of digital signatures. It was recalled that the Working Group, at its thirtieth session, had recognized that work with respect to certification authorities might be needed, and that such work would probably need to be carried out in the context of registries and service providers. However, the Working Group had also felt that it should not embark on any technical consideration regarding the appropriateness of using any given standard (ibid., para. 111). A concern was expressed that work on digital signatures might go beyond the sphere of trade law and also involve general issues of civil or administrative law. It was stated in response that the same was true of the provisions of the Model Law and that the Commission should not shy away from preparing useful rules for the reason that such rules might also be useful beyond the sphere of commercial relationships.

4. Another proposal, based on the preliminary debate held by the Working Group, was that future work should focus on service providers. The following were mentioned as possible issues to be considered with respect to service providers: the minimum standards for performance in the absence of party agreement; the scope of assumption of risk by the end parties; the effect of such rules or agreements on third parties; allocation of the risks of interlopers' or other unauthorized actions; and the extent of mandatory warranties, if any, or other obligations when providing value-added services (ibid., para. 116).

5. It was widely felt that it would be appropriate for UNCITRAL to examine the relationship between service providers, users and third parties. It was said that it would be very important to direct such an effort towards the development of international norms and standards for commercial conduct in the field, with the intent of supporting trade through electronic media, and not have as a goal the establishment of a regulatory regime for service providers, or other rules which could create costs unacceptable for market applications of electronic data interchange (EDI) (ibid., para. 117). It was also felt, however, that the subject matter of service providers might be too broad and cover too many different factual situations to be treated as a single work item. It was generally agreed that issues pertaining to service providers could appropriately be dealt with in the context of each new area of work addressed by the Working Group.

6. Yet another proposal was that the Commission should begin work on the preparation of the new general rules that were needed to clarify how traditional contract functions could be performed through electronic commerce. Uncertainties were said to abound as to what "performance", "delivery" and other terms meant in the context of electronic commerce, where offers and acceptances and product delivery could take place on open computer networks across the world. The rapid growth of computer-based commerce as well as transactions over the Internet and other systems had made that a priority topic. It was suggested that a study by the Secretariat could clarify the scope of such work. Should the Commission, after examination of the study, decide to pursue this task, one option would be to place such rules in the "Special provisions" section of the Model Law.

7. A further proposal was that the Commission should focus its attention on the issue of incorporation by reference. It was recalled that the Working Group had agreed that that topic would appropriately be dealt with in the context of more general work on the issues of registries and service providers (ibid., para. 114). The Commission was generally agreed that the issue could be dealt with in the context of work on certification authorities.

8. After discussion, the Commission agreed that placing the issue of digital signatures and certification authorities on the agenda of the Commission was appropriate, provided that it was used as an opportunity to deal with the other topics suggested by the Working Group for future work. It was also agreed as to a more precise mandate for the Working Group that the uniform rules to be prepared should deal with such issues as: the legal basis supporting certification processes, including emerging digital authentication and certification technology; the applicability of the certification process; the allocation of risk and liabilities of users, providers and third parties in the context of the use of certification techniques; the specific issues of certification through the use of registries; and incorporation by reference.

9. The Commission requested the Secretariat to prepare a background study of the issues of digital signatures and service providers, based on an analysis of laws currently being prepared in various countries. On the basis of that study, the Working Group should examine the desirability and feasibility of preparing uniform rules on the above-mentioned topics. It was agreed that work to be carried out by the Working Group at its thirty-first session could involve the preparation of draft rules on certain aspects of the above-mentioned topics. The Working Group was requested to provide the Commission with sufficient elements for an informed decision to be made as to the

scope of the uniform rules to be prepared. In view of the broad scope of activities covered by the Model Law and by possible future work in the area of electronic commerce, it was decided that the Working Group on Electronic Data Interchange would be renamed "Working Group on Electronic Commerce". [1/]

10. The Working Group on Electronic Commerce, which was composed of all the States members of the Commission, held its thirty-first session in New York from 18 to 28 February 1997. The session was attended by representatives of the following States members of the Working Group: Argentina, Australia, Austria, Bulgaria, China, Egypt, Finland, France, Germany, Hungary, India, Iran (Islamic Republic of), Italy, Japan, Kenya, Mexico, Poland, Russian Federation, Singapore, Slovakia, Spain, Thailand, Uganda, United Kingdom of Great Britain and Northern Ireland and United States of America.

11. The session was attended by observers from the following States: Canada, Colombia, Czech Republic, Denmark, Gabon, Indonesia, Ireland, Kuwait, Mauritania, Mongolia, Republic of Korea, Sweden, Switzerland and Turkey.

12. The session was attended by observers from the following international organizations: United Nations Conference on Trade and Development (UNCTAD), European Commission, International Bar Association (IBA), International Chamber of Commerce (ICC) and Union internationale des avocats (UIA).

13. The Working Group elected the following officers:

Chairman: Mr. Mads Bryde ANDERSEN (Denmark);

Vice-Chairman: Mr. PANG Khang Chau (Singapore);

Rapporteur: Mr. Piotr AUSTEN (Poland).

14. The Working Group had before it the following documents: provisional agenda (A/CN.9/WG.IV/WP.70), and a note by the Secretariat (A/CN.9/WG.IV/WP.71).

15. The Working Group adopted the following agenda:

1. Election of officers.

1/ Official Records of the General Assembly, Fifty-first Session Supplement No. 17 (A/51/17), paras. 216-224.

2. Adoption of the agenda.

3. Planning of future work on the legal aspects of electronic commerce: digital signatures, certification authorities and related legal issues.

4. Other business.

5. Adoption of the report.

I. DELIBERATIONS AND DECISIONS

16. The Working Group discussed the issues of digital signatures, certification authorities and related legal issues on the basis of the note prepared by the Secretariat (A/CN.9/WG.IV/WP.71). The deliberations and conclusions of the Working Group with respect to those issues are reflected in section II below. The Working Group also held preliminary discussions of the issues of incorporation by reference and future work. Those discussion are reflected in sections III and IV below.

II. LEGAL ISSUES AND POSSIBLE PROVISIONS TO BE CONSIDERED IN UNIFORM RULES ON DIGITAL SIGNATURES

A. General remarks

17. Before discussing possible provisions to be considered in uniform rules on digital signatures and related legal issues, the Working Group exchanged views on the scope of its work and considered initiatives currently being undertaken at the national level to address legal issues concerning digital signatures and certification authorities.

18. The Working Group heard reports on the efforts currently being made at the national level to address legal issues concerning digital signatures. A number of countries were considering the question of the appropriate legal regime for devices capable of performing, in an electronic environment, functions analogous to those of a handwritten signature in a paper-based environment. While in some countries the consideration of that question was still at its preliminary stages, it was reported that some countries had already enacted laws on digital signatures, or were in the process of preparing legislation on that subject against the background of the Model Law. Such legislation often contemplated the use of digital signatures based on public-key cryptography and certification authorities. The scope and level of detail of such legislation ranged from general laws adopted to enable the use of digital signatures as a method for authenticating electronic messages, to more detailed legislation that established a legal framework for the functioning of certification authorities and might also deal with a number of issues involving considerations of public policy, such as: the creation of the administrative framework required by a public-key infrastructure (PKI); the use of cryptography for digital signatures or for confidentiality purposes; issues of consumer protection;

and the possibility that government authorities would retain access to encrypted information, for example through a mechanism of "key escrow". The Working Group also heard reports on efforts towards harmonization that were currently undertaken at a regional level in a number of international organizations.

19. The question of the legal regime of devices used for performing functions equivalent to handwritten signatures, such as digital and other forms of electronic signatures, was found to be one of the most important issues that needed to be addressed so as to strengthen the legal infrastructure for electronic commerce. There was general agreement that the absence of a legal regime for digital and other electronic signatures might pose an impediment to economic transactions effected through electronic means. It was also agreed that the diversity of approaches and possible solutions being considered at the national level made that topic suitable for harmonization efforts on the part of UNCITRAL. In addition to providing guidance as to the legal framework to be established by enacting States with respect to digital and other forms of electronic signatures, it was felt that it would be useful for UNCITRAL to focus its work on the question of criteria for recognition of certificates issued by foreign certification authorities. It was suggested that UNCITRAL might also be in a position to facilitate that process by establishing internationally acceptable minimum standards for licensing certification authorities.

20. The Working Group considered the question whether its work should focus only on "digital signatures" (i.e., techniques involving the use of "public-key cryptography", also referred to as "dual-key cryptography") or whether it should also include other forms of electronic signatures. It was noted that technologies not based on public-key cryptography and generally referred to as "electronic signatures" were also being developed with a view to fulfilling functions typically performed by handwritten signatures. Those technologies included the use of codes or "passwords", or biometrical identification devices, and might coexist with a system of digital signatures based on a public-key infrastructure. It was noted that, in a paper-based environment, authentication and certification formalities and requirements were not needed in a number of transactions. While digital signatures within a public key infrastructure were said to afford a high degree of legal certainty, it was noted that other techniques might be found to provide useful identification and authentication methods in a variety of situations where such a high degree of legal certainty was not needed. The view was expressed that the Working Group should not create the erroneous impression that it discouraged the use of such other technologies by focusing only on digital signatures. In the context of that discussion, it was stated that the use of digital signatures relying on public-key cryptography did not necessarily imply that the highest degree of legal certainty was sought. Digital signature techniques were sufficiently flexible to provide also lower levels of security, thus involving lower costs.

21. It was widely felt that the aim of uniform rules on electronic signatures should be to provide guidance to legislators as to how a wide variety of authentication-related functions could be performed in an electronic environment. Such functions ranged along what was referred to as a "sliding scale" from providing the highest degree of security (along the lines of "notarized" and other certified signatures in a paper-based environment) to the low level of security offered by handwritten marks or signature stamps. However, one of the difficulties of undertaking work in the area of electronic signatures stemmed from the fact that, if the uniform rules to be prepared were to

provide the level of guidance that might be required to implement the principles embodied in article 7 of the Model Law, they might have to deviate from a purely functional approach, and to address in some detail the manner in which specific techniques could perform the above-mentioned functions.

22. There was general agreement that, consistent with media neutrality in the Model Law, the uniform rules to be developed by the Working Group should not discourage the use of any technique that would provide a "method as reliable as appropriate" as an alternative to handwritten and other paper-based signatures in compliance with article 7 of the Model Law. However, with a view to facilitating its deliberations, the Working Group decided that the focus of its work would be placed initially on issues of digital signatures, which were better known than other techniques, through legislation and legal literature. It was generally understood that, where appropriate in the discussion, a more general approach could be taken, and issues relevant to other electronic signature techniques could also be considered.

23. As to the scope of its work, there was general agreement in the Working Group that it should not extend to questions relating to the use of cryptography for security purposes. Those questions, which were already being considered at other international forums, such as the Organization for Economic Cooperation and Development (OECD), were of great complexity, were not directly relevant to the implementation of a digital signature scheme, and could compromise the progress of the deliberation of the Working Group, which should focus its work on facilitating electronic commerce. More generally, it was agreed that the uniform rules to be prepared should not attempt to deal with any of the issues of national security, public policy, criminal or administrative law that might become involved in the implementation of digital signature schemes.

24. Various views were expressed as to whether the Working Group should also address consumer law issues. According to one view, consumer issues should be excluded from the scope of the current work, which should instead focus exclusively on commercial transactions. Another view was that, while the main issues to be considered were not intrinsically consumer-related, it might be appropriate to consider, in the preparation of uniform rules on digital signatures, whether different standards were needed for consumer transactions. It was suggested, however, that making specific provisions for consumer law issues might prove particularly difficult because the nature of electronic communications made it almost impossible to identify any party as a consumer. After discussion, it was agreed that, while focusing primarily on commercial transactions, the Working Group would take note of possible implications of the matters it discussed with respect to consumer transactions.

B. Specific legal issues and draft provisions on digital signatures

25. As to the form of the work to be undertaken by the Working Group, various views were expressed. One view was that it would be premature to consider that the work to be prepared by the Working Group on the issues of digital signatures and related issues should take the form of model legislation. Another view was that, as a working assumption, the Working Group should decide that its future work on the issues of digital signatures and related issues should be regarded as an addition to the Model Law. It was recalled that, at its twenty-ninth session, the Commission had requested the Working Group to examine the desirability and feasibility of preparing uniform rules on the issues of digital signatures and certification authorities. The Commission had agreed

that work to be carried out by the Working Group at the current session could involve the preparation of draft rules on certain aspects of the above-mentioned topics (see above, para. 9).

26. After discussion, the Working Group postponed its decision as to the form of its future work until it had completed its review of the substantive legal issues involved. The Working Group also postponed its consideration of the precise relationship between such future work and the Model Law. It was agreed that possible uniform rules in the area of digital signatures should be derived from article 7 of the Model Law and should be considered as setting out a manner in which a reliable method could be used "to identify a person" and "to indicate that person's approval" of the information contained in a data message. More generally, future work on digital signatures should be consistent with the principles expressed, and the terminology used, in the Model Law.

27. To assist in its discussions in the future, the Working Group adopted as a tentative working assumption that its work in the area of digital signatures would take the form of draft statutory provisions. The view was expressed, however, that the Working Group might consider the need to provide additional explanations, possibly by way of a preamble, by way of a guide to enactment of the uniform statutory provisions, or through the elaboration of separate guidelines, in particular with respect to issues that might be regarded as unsuitable for unification. For example, it was stated that illustrative comments emanating from UNCITRAL regarding the various issues raised by the establishment of public-key infrastructure might play a useful educational purpose.

28. It was decided that the Working Group would proceed with its deliberations on the basis of the draft uniform provisions set forth in the note by the Secretariat (A/CN.9/WG.IV/WP.71, paras. 52-76). It was noted that those draft provisions were very tentative in nature, and it was generally agreed that the review of those draft provisions, rather than focusing on the drafting of each individual article, should be regarded as an opportunity to discuss the conceptual approach on which uniform rules on digital signatures could be based. It was generally felt that, in the context of its discussion of each of the issues addressed by the draft provisions, the Working Group might need to consider: (a) whether uniformity was needed; (b) whether the issue was sufficiently treated in the Model Law or whether more detailed provisions were desirable; (c) whether the issue was specific to digital signatures or whether it could be dealt with at a more general level; (d) whether the issue was directly relevant to international trade law, to the mandate of UNCITRAL and to its field of expertise; and (e) whether a mandatory rule was needed or whether party autonomy should prevail.

1. Definitions

29. At the outset, the view was expressed that, in addition to the draft definitions of "digital signature", "authorized certification authorities" and "certificates" set forth in the note by the Secretariat (A/CN.9/WG.IV/WP.71, paras. 52-60), the Working Group might need to consider additional definitions. The following definitions were suggested: "'private key' means the key of a key pair used to create a digital signature"; "'public key' means the key of a key pair used to verify a digital signature"; "'key pair', in an asymmetric cryptosystem, means a private key and its mathematically-related public key, having the property that the public key can verify a digital signature that the private key creates". The Working Group took note of the suggestion. The view was expressed that the suggested definitions might be somewhat circular. More generally, a note of

caution was struck about introducing a large number of definitions in uniform rules of a statutory nature, which might be contrary to the legislative tradition in many countries. After discussion, it was generally agreed that the possibility of adding a limited number of definitions might need to be reconsidered at a later stage.

(a) Digital signature

30. The Working Group discussed the definition of "digital signature" on the basis of the following draft provision:

"Draft article A

"(1) A digital signature is a numerical value, which is affixed to a data message and which, using a known mathematical procedure associated with the originator's private cryptographic key, makes it possible to determine uniquely that this numerical value has been obtained with the originator's private cryptographic key.

"(2) The mathematical procedures used for generating authorized digital signatures under [this Law][these Rules] are based on public-key encryption. When applied to a data message, those mathematical procedures operate a transformation of the message such that a person having the initial message and the originator's public cryptographic key can accurately determine

"(a) whether the transformation was operated using the private cryptographic key that corresponds to the originator's public cryptographic key; and

"(b) whether the initial message was altered after the transformation was made.

"(3) A digital signature affixed to a data message is regarded as authorized if it can be verified in accordance with procedures laid down by a certification authority authorized under [this Law] [these Rules].

"(4) The [relevant authority in the enacting State] shall lay down specific rules for the technical requirements to be met by digital signatures and the verification thereof."

Paragraphs (1) and (2)

31. The view was expressed that the definition of "digital signature" should be extended to cover not only the use of public-key cryptography but also other types of electronic signatures. The prevailing view, however, was that it would be inappropriate to attempt creating a definition of "digital signature" that would depart from existing usages. It was agreed that, while the notion of "digital signature" should be restricted in scope to cover only asymmetric cryptography, other definitions might be needed to cover other techniques that might be broadly referred to under the notion of "electronic signatures".

32. With respect to paragraph (1), it was suggested that the words "to determine uniquely that this numerical value has been obtained" should be replaced by the words "to determine that this numerical value has only been obtained". The Working Group decided that, at such an early stage of its deliberations, it should not engage in any detailed redrafting of the text. It was generally felt that paragraphs (1) and (2) reflected in substance the notion of "digital signature" as it might be used to delimit the scope of future work. After discussion, the Working Group found the substance of paragraphs (1) and (2) to be generally acceptable, but agreed that it might need to reconsider their specific drafting at a later stage.

Paragraph (3)

33. Various questions were raised concerning the purpose of paragraph (3). The view was expressed that paragraph (3) was inadequate for the purpose of introducing the notions of public-key infrastructure and verification of digital signatures and that paragraph (3) dealt instead with substantive matters that did not belong in the definition of "digital signature". The view was expressed that paragraph (3) might be read as introducing a verification procedure as a requirement for the validity of a digital signature. It was suggested that it would be preferable to delete paragraph (3) and replace it with a descriptive definition of "verification" of signatures.

34. It was pointed out that paragraph (3) might be read as dealing only with the validity of digital signatures that were used in the context of a public-key infrastructure implemented by public authorities. As currently drafted, that provision was felt to be excessively rigid, as it might preclude the recognition of the use of digital signatures in any other context, such as public-key infrastructures implemented by entities other than public authorities. It was generally felt that it would be undesirable to affect transactions that might take place in closed circles between parties that did not feel the need for obtaining the services of a certification authority. At a time when various options for public-key infrastructure were still under consideration by States, it was stated that it would be premature to make a choice in the draft uniform rules in favour of any particular system of public-key infrastructure to the detriment of all others.

35. The view was expressed that, while paragraph (3) had to be read in conjunction with article 7 of the Model Law, the two provisions might not be entirely consistent with one another. For instance, paragraph (3) qualified the notion of "digital signature" by referring to "authorized" digital signature, a word that was not used in the context of article 7 of the Model Law or elsewhere in draft articles A to J as set forth in the note by the Secretariat (A/CN.9/WG.IV/WP. 71). Moreover, article 7 of the Model Law referred to the use of a signature method "as reliable as was appropriate for the purposes for which the data message was generated or communicated", thus admitting varying levels of reliability according to the purposes for which the data message was generated or communicated, including any agreement of the parties. It was pointed out that, under article 7 of the Model Law, the parties to a transaction having sufficient confidence in one another could agree to a level of security they found appropriate in the circumstances, without necessarily resorting to a certification authority. From the parties' perspective, the essential consideration was whether they regarded the system they operated as trustworthy. A number of factors were said to make up for the trustworthiness of the hardware, software and procedures used by the parties (e.g., whether they were reasonably secure from intrusion and misuse; whether they provided a reasonable level of availability, reliability and correct operation; whether they were reasonably suited to performing

their intended function, and whether they were operated in conformity with generally accepted security principles). Therefore, it was for the parties to decide whether the standard of reliability they required should include a verification procedure applied by a certification authority. Paragraph (3), in turn, implied that digital signatures would only be reliable if they were capable of being certified with the assistance of a certification authority. It was therefore found to be more restrictive than article 7 of the Model Law. It was stated that substantive revision would be required if paragraph (3) was to be brought into harmony with article 7 of the Model Law.

36. Questions were also raised concerning the reference, in paragraph (3), to verification of the digital signature in accordance with procedures laid down by the certification authority. The view was expressed that a reference to those procedures raised the issue of the technical instructions applied for verification of digital signatures and other operation criteria observed by the certification authority, or the legal effects that would flow from those procedures not being followed in a given case. However, those were substantive questions which could not properly be dealt with within the limited scope of draft article A. Therefore, it was suggested that the reference to verification procedures should be deleted from paragraph (3).

37. Having considered the different views expressed, the Working Group decided to delete paragraph (3). It was agreed that the discussion of possible options of public-key infrastructure might need to be reopened after the question of the legal effects of digital signatures had been examined.

Paragraph (4)

38. The view was expressed that, to the extent it required the State to lay down technical rules for digital signatures, paragraph (4) appeared to exclude public-key infrastructures implemented by entities other than public authorities. Consistent with its decision to delete paragraph (3), and given the logical relation between the two provisions, the Working Group decided that paragraph (4), too, should be deleted.

(b) Authorized certification authorities

39. The Working Group discussed the definition of "authorized certification authority" on the basis of the following draft provision:

"Draft Article B

"(1) The ... [the enacting State specifies the organ or authority competent for authorizing certification authorities] may grant authorization to certification authorities to act in pursuance of [this Law] [these Rules]. Such authorization may be revoked.

"(2) The ... [the enacting State specifies the organ or authority competent to promulgate

regulations with respect to authorized certification authorities] may establish rules governing the terms under which such authorizations may be granted and promulgate regulations for the operation of certification authorities.

"(3) Authorized certification authorities may issue certificates in relation to the cryptographic keys of natural and legal persons.

"(4) Authorized certification authorities may offer or facilitate registration and time stamping of the transmission and reception of data messages as well as other functions regarding communications secured by means of digital signatures.

"(5) The ... [the enacting State specifies the organ or authority competent to lay down specific rules with respect to the functions to be performed by authorized certification authorities] may lay down more specific rules for the functions to be performed by authorized certification authorities in connection with the issuance of certificates to individual natural or legal persons."

40. The Working Group held a general exchange of views on the approach that should be taken for dealing with certification authorities. Pursuant to one view, draft article B, as currently formulated, appeared to prescribe a specific method for implementing a public-key infrastructure and it would be preferable to leave it for each enacting State to adopt its own rules on that matter. It was stated that, while certification authorities might play an essential role in building trust in the reliability of digital signatures, digital signature systems functioning in the absence of certification authorities were not inconceivable. It was also stated that the establishment of a public law scheme under which certification authorities might be authorized to operate would not necessarily foster the trustworthiness of digital signatures, which might be better achieved through privately-appointed certification authorities, or other forms of market-driven mechanisms. Another view was that draft article B was generally acceptable for the purpose of defining certification authorities, since it was formulated in a permissive way, in particular through paragraph (2), which did not prevent the enacting State from implementing its public-key infrastructure in a different fashion.

41. For the purpose of considering possible approaches that should be taken for dealing with certification authorities, the Working Group was invited to consider two possible objectives that might be pursued through a definition of "certification authority". One objective might be to provide guidance to enacting States concerning essential elements to be considered when implementing national public-key infrastructures. It was stated that draft article B was not sufficiently detailed to provide adequate guidance in that regard. An alternative objective might be to leave the internal implementation of public-key infrastructures to each enacting State, while setting forth in the definition of "certification authority" the criteria to be applied by each enacting State for the recognition of certificates issued by foreign certification authorities. It was suggested that, should the Working Group wish to circumscribe the scope of the draft uniform rules to the latter purpose, an opening paragraph might need to be inserted in draft article B along the following lines: "These uniform provisions apply to certificates issued pursuant to a legal regime having the following attributes:". It was noted, however, that, if adopted, such a proposal would require substantive revision of the remaining provisions of draft article B. Another suggestion was that no

specific criteria should be set forth under draft article B, which should be limited in that respect to the general statement contained in paragraph (2). Additional comments, including an illustrative list of possible criteria to be taken into account by enacting States, might be provided in a guide to enactment of the draft uniform rules.

42. The Working Group agreed that the question whether a definition of "certification authority" was needed in the draft uniform rules for purposes other than defining the criteria to be applied by each enacting State for the recognition of certificates issued by foreign certification authorities might need to be discussed further at a later stage. It was widely felt that, while the establishment of standards or criteria might help certification authorities in generating the level of trust necessary to their operation, it might be necessary to distinguish between the general issues of trustworthiness of certification authorities, which might depend upon the legal regime under which they were established, and the more specific issues related to the level of trust generated by the individual certificates issued by the certification authority.

43. The view was expressed that provisions concerning the functions and duties of certification authorities, such as set forth in draft article B, were not only relevant as structural elements of a system of certification authorities (e.g., a public-key infrastructure). Provisions of that type were also relevant for the purpose of determining the effects to be granted to digital signatures and acts related to, or involving the use of, digital signatures. Against that background, it was suggested that, in its deliberations on that matter, the Working Group might benefit from bearing in mind a spectrum of factors relevant for determining the legal effects to be granted to digital signatures. The following factors were offered as an analytic tool for consideration by the Working Group: (a) types of signature (which, in decreasing order of generality, included electronic signatures; digital signatures; digital signature with certificate and digital signature with certificate from a publicly authorized certification authority); (b) parties affected (i.e., immediate contracting parties, including certification authorities; third parties such as shippers and banks; governmental entities; other persons such as service providers, communications carriers); (c) acts or events to be given legal effect (i.e., the use of digital signature; the issuance of a certificate, including unauthorized issuance; the expiration of a certificate; the revocation of a certificate; the revocation of an authorization given to a certification authority); (d) scope of the work of UNCITRAL in that area (international application only; international application plus proposals for domestic laws; proposals for domestic laws); (e) legal effect (i.e., validity; obligations of issuer of certificates and of person relying on certificates; remedies; liability, including limits to liability; evidence); (f) drafting techniques (i.e., prescription of standards; legal effect if standards were met; legal effect if standards were not met). The Working Group considered the proposed list of factors to be a useful instrument to facilitate its analysis of the purpose and implications of provisions concerning certification authorities.

44. In its ensuing discussions, the Working Group examined the question whether it would be desirable for the draft uniform rules to include operation criteria to be met by certification authorities, whether authorized or not.

45. It was suggested that, in addition to the provisions it already contained, draft article B should be supplemented with uniform rules expressly mentioning the criteria which should be taken into account when authorizing certification authorities to operate or otherwise defining the minimum standards to be met by certification authorities in order to achieve legal recognition of the

certificates they issued. Reference to such criteria was necessary if the draft uniform rules were to deal with certification authorities. It was recalled that paragraph 44 of the note by the Secretariat (A/CN.9/WG.IV/WP.71) listed a number of factors that might be taken into account when assessing the trustworthiness of a certification authority. It was generally found that such a list constituted a good basis for discussion, should the Working Group wish to consider the matter further. It was suggested that some of those criteria might be expanded so as to encompass factors such as the competence of the personnel at the managerial level or the isolation of the certifying function from any other business that the certification authority might pursue.

46. Objections were voiced to the inclusion of operation criteria for certification authorities in the draft uniform rules. The Working Group was reminded of its earlier discussion concerning the role of public authorities in the implementation of public-key infrastructures and the possibility that in some States private entities would exercise certifying functions without requiring prior governmental authorization (see above, para. 40). Also, other acceptable alternatives to governmentally-approved criteria might be considered, such as internationally-recognized commercial usages and practices or qualification standards developed by reputable non-governmental entities, as was the case in certain fields of commercial activities. It was felt that the proposed inclusion of criteria to be taken into account when authorizing certification authorities to operate would be neither relevant nor appropriate in the case of certification authorities that did not operate pursuant to a governmental authorization. Furthermore, the inclusion of any such criteria would make it necessary to identify the entity or authority competent for establishing whether any particular certification authority met the said criteria. Such a system would lead to difficulties in the case of certification authorities that operated outside a public-key infrastructure implemented by public authorities.

47. In response to those objections, it was recalled that the provision of commonly accepted criteria for the operation of certification authorities might be an important step towards enhancing the trustworthiness of digital signatures. Such criteria might not be needed as long as electronic transactions took place between parties operating within a closed system which they regarded as being reasonably reliable. Trusted partners operating in such closed systems might in fact dispense with certificates issued by certification authorities. However, in order to allow for a wider use of digital signatures, it would be necessary to promote the confidence of the general public in the authenticity of the signatures and in the reliability of the methods being used for their verification. One important way of achieving that purpose was to satisfy the general public that entities engaging in the business of certifying the authenticity of a public key had to meet certain criteria devised to ensure their trustworthiness. While the Working Group should not discard the possible role of commercial usages and practices, or of non-governmental entities in developing acceptable operation standards for any particular field of commercial activity, it was noted that no established practice had yet evolved for determining acceptable operation criteria for certification authorities.

48. It was suggested that the two alternatives under debate, namely the establishment of criteria for a governmental authorization of certification authorities and the recognition of operation criteria for certification authorities functioning outside a governmentally-implemented public-key infrastructure, might not be mutually exclusive. The difference between those two situations might reside in the legal effects given to digital signatures in one or the other case. In the case of governmentally-authorized certification authorities, the fulfilment of the applicable operation criteria by a certification authority would constitute a prerequisite for the authorization of that certification

authority, which, in turn, would be a condition for the recognition of the legal effectiveness of the certificates issued by that certification authority. In the second situation, a certification authority would not need to demonstrate that the operation criteria were met prior to beginning to function. However, if the certificates it issued were to be challenged (e.g., in a judicial dispute or arbitration), the adjudicating body would need to assess the trustworthiness of the certificate by determining whether it had been issued by a certification authority meeting those criteria.

49. A view was expressed that the trustworthiness of a certificate might depend on the actions of a certification authority with respect to that particular certificate, not on institutional factors. Such "transactional" trustworthiness would not necessarily depend on the authorized or non-authorized nature of the certification authority or on internationally-recognized commercial usages and practices. It was suggested that the criteria of trustworthiness would depend on the purpose for which trustworthiness was assessed (e.g., cross-certification, the granting of a license, determination of liability).

50. Given the early stage of its deliberations and the conflicting views expressed on that subject, there was general support to the proposal that the Working Group should keep the above-mentioned suggestions as possible working assumptions and should revert to those issues at a later stage, after considering other questions intrinsically related thereto, such as the question of the liability of certification authorities and issues of cross-border certification.

2. Liability

51. The Working Group based its discussion of the liability of certification authorities on the following draft provision:

"Draft article H

"(1) An authorized certification authority shall be liable to any person who has acted in good faith in reliance on a certificate issued by the certification authority for any loss due to defects in the registration of the certification authority, technical breakdowns or similar circumstances [even if the loss is not due][if the loss is due] to negligence by the certification authority.

"(2) Variant X The liability for any individual loss shall not exceed [amount]. The ... [the enacting State specifies the organ or authority competent to revise the maximum amount] may regulate this amount every second year to reflect price developments.

Variant Y The ... [the enacting State specifies the organ or authority competent to promulgate liability regulations] may promulgate regulations on the liability of certification authorities.

"(3) In case the party who has sustained the loss has contributed to this wilfully or negligently, the compensation may be reduced or may not be granted.

"[(4) Where an authorized certification authority has received notice of revocation of a certificate, the authority shall register such revocation forthwith. If the authority fails to do so, it shall be liable for any resulting loss sustained by the user.]"

Paragraphs (1) and (2)

General remarks

52. The Working Group engaged in a discussion concerning the scope and implications of the proposed rules on the liability of certification authorities. It was stated that the issue of liability of certification authorities involved two different types of liability: a "structural" liability, which resulted from the breach by the certification authority of its terms of operation, and a "transactional" liability, which resulted from the certification authority's actions in issuing, suspending or revoking a certificate. In the first case, the certification authority was in breach of the public confidence placed upon it, and it would be appropriate for the authorizing public entity to levy fines or impose other sanctions, commensurate with the gravity of the violation. In the second case, the certification authority was in breach of its professional obligations to its own customer. However, the loss would often be sustained by the latter's trading partner, who in most cases would not have a contractual relationship with the certification authority. Under those circumstances, it was asked whether it would be appropriate for the injured party to have direct recourse against the certification authority, or whether the injured party should have a right of redress against its trading partner only, who, in turn, might have recourse against the certification authority. It was suggested that it would be difficult to establish an adequate regime of liability in which the user of a certificate would have direct recourse against the certification authority.

53. The view was expressed that it might be preferable for the Working Group to avoid dealing with the liability of certification authorities, since that was a delicate and complex issue that could not adequately be dealt with in the draft uniform rules. It was recalled that, within the context of the Model Law, it had been decided to avoid the issue of liability of third-party service providers altogether. It was suggested that the question of liability was closely related to the question of damages, which might not easily lend itself to international harmonization. The Working Group was invited to consider whether it would be more appropriate to exclude both questions from the scope of the draft uniform rules and leave them for the applicable national law. If such an approach was to be adopted, the following alternatives could be considered: to leave it for national conflict-of-laws rules to determine the law applicable to the questions of liability and damages; to draft a specific uniform conflict-of-laws rule; or to determine directly which conflict-of-laws rule should be applied (e.g., the conflict-of-laws rule of the country in which the certification authority was registered or otherwise authorized to do business). In support of that suggestion it was stated that the question of liability was essentially a question of the warranties provided by the certification authority, which was best left for the contracting partners to regulate, or should be determined in accordance with the national law that applied to their contractual relationship.

54. Strong support was expressed, however, for including provisions on the liability of certification authorities in the draft uniform rules. The issue of liability was described as too important to be left entirely for the parties to regulate, particularly in view of the fact that not all

users of certificates might be in a direct contractual relationship with the certification authority. Limiting the user's rights to seeking redress from its trading partner for failures by the certification authority would leave unprotected those persons who were victims of fraudulent acts involving the use of fictitious names or identities with the knowledge or the contributory negligence of the certification authority. Furthermore, the lack of uniform rules on the liability of certification authorities might lead to the undesirable situation in which some countries would only provide a derisory level of liability with a view to attracting or fostering the establishment of certification authorities on their territories. The possible emergence of "certification heavens" might generate reluctance on the part of trading partners when considering the use of digital signatures, a situation which would not be in keeping with the objective of promoting electronic commerce. However difficult the subject might be, involving aspects of both contractual and tortious liability, the prevailing view was that the question of the liability of certification authorities should be dealt with in the uniform rules.

55. After discussion, the Working Group agreed that, in principle, the draft uniform rules should contain provisions regarding the liability incurred by certification authorities in the context of their participation in digital signature schemes.

Nature of liability

56. Questions were raised concerning the nature of the liability of the certification authority, in particular whether such liability would be based on negligence or whether it would be defined as "strict liability", a notion which was also referred to as "objective liability" or "no-fault liability". Objections were raised to the inclusion of provisions making the certification authority strictly liable. It was stated that strict liability was a deviation from the general principle of tort law whereby a person was liable for his or her own negligence and, as such, was accepted in national law for exceptional reasons of public interest, such as certain strict liability regimes of persons conducting unreasonably hazardous activities. There was no compelling reason why certification authorities should be subject to a regime of strict liability. Moreover, such a regime would have the undesirable consequence of discouraging the emerging industry of certification authorities, thus limiting the possibilities of use of digital signatures. Furthermore, it was observed that certification authorities might provide different levels of service to their clients and to the general public, ranging from simply listing names of public key holders and their respective keys to more individually-tailored services involving guarantees of the authenticity of public keys and the identity of their holders. The level of obligation assumed by certification authorities as well as the fees they charged varied according to the type of service they provided. Bearing such a range of services in mind, it would not be reasonable to impose the same level of liability upon all certification authorities in all conceivable circumstances. It was thus suggested that the regime of liability applicable to certification authorities should be based on negligence, under one option provided under paragraph (1) of draft article H.

57. In response, it was observed that it would not be equitable to require that the injured party should bear the burden of establishing the negligence of the certification authority. Given the high level of technical sophistication that might be expected from certification authorities and the high level of trust they were intended to generate, certification authorities should, in normal circumstances, be held liable whenever the issuance of faulty certificates resulted in damages. It was

pointed out that, in some legal systems, certain professional categories (e.g., notaries public in certain civil law countries) were under an obligation to purchase third-party liability insurance or to participate in a common compensation fund for indemnifying parties injured as a result of their acts. It was suggested that the establishment of such a common compensation fund might be facilitated if certification authorities were to be organized within an institutional framework such as a licensing scheme.

58. It was suggested that the divergence of views expressed in the Working Group might be solved if, instead of a positive rule specifying the circumstances under which the certification authorities would be liable, the draft uniform rules contained a rule establishing a rebuttable presumption of liability. Under such a proposal, for example, in the event of erroneous identification of a person or erroneous attribution of a public key to a person, the certification authority would be held liable for the loss sustained by any injured party, unless the certification authority could demonstrate that it had done its best efforts to avoid the error. The certification authority could rebut the presumption, for example, by demonstrating that it had adhered to a standard of conduct that might be established by the uniform rules. It was noted that such a liability scheme, which was similar to schemes contemplated in some national laws concerning product liability, would provide additional protection to service users, without however imposing strict liability on the certification authority. The Working Group welcomed that proposal, which was generally felt to provide a viable approach for future consideration of the Working Group in dealing with the difficult issue of liability of certification authorities.

59. The Working Group proceeded to consider the circumstances that could excuse a faulty performance by the certification authority. It was suggested that, under the proposed liability scheme, the certification authority should be exempt from liability if it could demonstrate that it exercised reasonable care in identifying the public key holder or performing its authentication functions; that the errors resulted from the user's own fault, as indicated in paragraph (3) of draft article H; or that the error was attributable to circumstances beyond the certification authority's control. It was generally felt that exempting events along those lines would be acceptable.

Certification practice statements and party autonomy

60. The view was expressed that in considering the issue of liability it was important to bear in mind the mutual expectations and interests of the user and the certification authority. The certification authority should be expected to disclose its certification practice statement (CPS), apprising the users, inter alia, of the methods and procedures it used for identifying the holder of public key. The user should be expected to reasonably ascertain that document. Moreover, users should have the duty to ascertain the current validity of a certificate (e.g., that the certificate had not been revoked) prior to relying on a certificate. Finally, users should be expected to act reasonably on the basis of the information available to them. To questions that were raised as to how the users could verify the validity of a certificate, it was replied that certification authorities could be required to maintain databases of valid certificates, as some already did, which would be accessible to interested parties for the purpose of verifying the validity of certificates. In response to that proposal it was suggested that, while it might be appropriate to encourage the users' diligence in dealing with certificates, the primary responsibility for the authenticity and validity of a certificate rested with the certification authority and great caution should be exercised prior to imposing duties

on the users which might make them share that responsibility. In most cases, the users would not normally be in a position to ascertain a number of factors relevant to the validity of a certificate, such as the identification procedures used by the certification authority, or whether the holder of the public key also held the corresponding private key. It would not be reasonable to shift any of those responsibilities to the user.

61. The Working Group engaged in a discussion of the role of certification practice statements and the extent to which they could play a role in limiting or otherwise defining the scope of the liability assumed by certification authorities. For the purpose of protecting users' interests, certification authorities could be required to disclose the extent of such liability by means of corresponding provisions in the certification practice statements they issued. From a technological point of view, certification practice statements could be accessible in electronic form to persons using the services of a certification authority. The view was expressed that a party who requested the services of a certification authority should accept to be bound by the terms of a certification practice statement by making use of the services of a certification authority. Contractual arrangements entered into between the parties should take precedence over rules coming from other sources, and in that connection it was important to ensure the enforceability of those terms and conditions. It was suggested, however, that provisions as important to the relying parties as a limitation of liability should appear in the certificate itself and not merely in a document referred to in the certificate, however accessible that document might be.

62. It was widely felt in the Working Group that in devising a liability scheme for certification authorities due regard should be had to the need to preserve party autonomy. Reservations were expressed, however, about the possibility that a certification authority might avoid liability for its own negligence by virtue of liability exemption clauses or disclaimers contained in the certification practice statement or in any other document issued by that certification authority. It was stated that the receiver of a message who used a certificate to verify the authenticity of a digital signature often would not have a direct legal relationship with the certification authority and therefore would not be in a position to negotiate with the certification authority the terms of such liability provisions. Even the issuer of the message, who was in a privity relation with the certification authority, might not always be able to negotiate those terms, which in many cases would take the form of pre-established business conditions not open to amendments. In some legal systems a unilateral exclusion of limitation of liability would be contrary to public policy. If introduced, liability limits and exemptions should be pursuant to the law or should be approved by public authorities.

Limits of liability

63. The Working Group considered the question whether the liability of certification authorities should be subject to limits and how such limits could be established. As an objection to introducing liability limits for certification authorities, it was observed that such limits usually existed in fields of activity subject to some form of monopoly, as was the case of postal and telephonic services in a number of countries. However, in other fields of activity open to competition, there was no reason for such liability limits.

64. Various views were expressed, however, in support of establishing some form of limitation to

the liability of certification authorities. The following points were made: (a) certification authorities constituted an emerging industry, the development of which might be hampered by exposing them to open-ended liability; (b) it was important to make it possible for certification authorities to determine the level of liability they were ready to assume and it might be a precondition to enable them to contract for adequate insurance coverage of their activities; and (c) it might happen that, with respect to digital signatures, the role of a certification authority would be limited to issuing a certificate, which in itself might have little or no quantifiable value. It was further stated that, where a certificate was issued to establish a link between a public key and a given individual, that certificate might be appended to a number of messages in a variety of different transactions, the total amount of which would in most cases be unforeseeable for the certification authority. It was pointed out that, in the case of credit card transactions, there existed means for authorizing each transaction individually, so that the credit card company could, for each instance where a credit card was used to conclude a transaction above a predetermined amount, estimate its potential liability in case of unauthorized use of the credit card. Such a possibility did not exist for certification authorities, which were normally unaware of the terms of the transactions carried out by their clients. Therefore, it would be difficult to establish a threshold or ceiling of liability by reference to the amount of the transaction for the purpose of which a digital signature was used. Given the infinite number of transactions to which one single certificate might relate, it was doubtful that certification authorities would be in a position to acquire third-party liability insurance at a reasonable cost.

65. With regard to the possible methods for limiting the amount of the liability incurred by certification authorities, a number of suggestions were discussed by the Working Group. One possible approach would be to determine a fixed amount, as suggested in variant X of paragraph (2) of draft article H. Other suggested approaches relied on a limitation of the liability by reference to a multiplier of the fee paid by the subscriber, a percentage of the transaction value or a percentage of the actual loss sustained by the injured party. It was pointed out, however, that the damage that might result from the acts of a certification authority was not easily quantifiable, so as to serve as an objective criterion for arriving at a fixed amount of liability. Also, the service rendered by a certification authority, and the fees it charged, often bore no relationship to the value of the transactions to which they related or to the damage that might be sustained by the parties. Other limitation schemes, such as the ones contained in the United Nations Convention on the Carriage of Goods by Sea (the Hamburg Rules) or in the UNCITRAL Model Law on International Credit Transfers, concerned transactions that involved quantifiable elements (e.g., the value of the goods, the amount of the credit transferred) that might not exist in the case under consideration.

66. Another possibility for limiting the liability consisted in excluding liability for certain types of damages, such as "consequential" damages. With regard to the latter possibility, it was observed that the notion of "consequential damages", which was also referred to as "indirect damage", might be given different interpretations in different legal systems. It was thus suggested that it would be preferable to mention specifically the types of losses encompassed by that notion in respect of which the certification authority would not assume liability. While support was expressed in favour of developing an approach that would result in excluding liability for consequential damages, consistent with the approach taken by the UNCITRAL Model Law on International Credit Transfers, it was pointed out that such an approach might not be appropriate in the context of digital signatures and certification authorities. It was stated that damage would rarely result directly from the issuance of, for example, a fraudulent certificate, but rather from third-party reliance on an unreliable digital

signature using such a certificate. To that extent, most conceivable damages resulting from the activities of certification authorities might be regarded as "consequential" or "indirect". A further suggestion was to use the element of "foreseeability" as a criterion for limiting the liability of certification authorities. It was stated that the liability regime applicable to the seller of goods under the United Nations Convention on Contracts for the International Sale of Goods might need to be further explored as a possible point of reference.

67. Having regard to the variety of alternatives suggested, the Working Group requested the Secretariat to prepare a brief report on existing legal regimes and methods used for limiting liability, particularly under international conventions applicable to the transport of goods and the transport of passengers. Such a report could also examine the liability regime established under certain national laws for professional categories performing, in a paper-based environment, functions akin to those contemplated for certification authorities.

Minimum standard of liability

68. It was noted that, at the current stage of its deliberations, the Working Group was still considering whether certification authorities should require prior authorization from a public entity. It was suggested that, when reverting to that issue in the context of its continued discussion of draft article B, the Working Group should also consider whether such authorizing public entity would be subsidiarily liable for the acts of the certification authority.

69. With respect to paragraphs (1) and (2), the Working Group adopted as a provisional conclusion that the liability regime applicable to certification authorities should be based on a "dual approach", namely, that it should recognize that liability might vary depending on whether a certification authority had standards imposed on it by a public entity, or whether it merely functioned on the basis of privately-agreed standards.

70. It was suggested that any certification authority, when issuing a certificate, should be under an obligation which might read as follows:

"By issuing a certificate, a certification authority represents that it has confirmed that:

"(1) the certification authority had complied with all applicable requirements of these Rules in issuing the certificate, and if the certification authority has published the certificate or otherwise made it available to any person who reasonably relies on the certificate or a digital signature verifiable by the public key listed in the certificate, that the holder listed in the certificate has accepted it;

"(2) the holder identified in the certificate holds the private key corresponding to the public key listed in the certificate;

"(3) the holder's public key and private key constitute a functioning key pair;

"(4) all information in the certificate is accurate, unless the certification authority has stated in

the certificate [or incorporated by reference in the certificate] a statement that the accuracy of specified information is not confirmed;

"and

"(5) to the certification authority's knowledge, there are no known, material facts omitted from the certificate which would, if known, adversely affect the reliability of the foregoing representations."

It was generally agreed that the suggested wording was, for the most part, acceptable in substance as the basis for future discussions, as setting a minimum standard from which the parties should not be allowed to derogate by private agreement. In particular, no clause limiting the liability of a certification authority should be considered within the scope of any protection or benefit provided by the uniform rules if it conflicted with the above-mentioned requirements. Where the liability of a certification authority was alleged, the certification authority would be presumed to be liable for the consequences of issuing a certificate, unless it could prove that it had met the above-mentioned requirements. However, should a certification authority wish to undertake obligations stricter than the above-listed representations, it should be allowed to do so, by way of clauses included in a certification practice statement or otherwise.

71. The Working Group agreed that the above-mentioned minimum standard should be applicable to the issuance of certificates for the purposes of digital signatures, as defined in draft article A. It was generally agreed that the draft uniform rules should not attempt to deal with other activities or services that might be performed by certification authorities. Such activities and services might be subject to any contractual arrangement between certification authorities and their customers, and to any other applicable law (e.g., mandatory rules of law regarding the acceptability of liability exemption clauses).

Paragraphs (3) and (4)

72. The Working Group found the substance of paragraphs (3) and (4) to be generally acceptable as a basis for future discussions. With respect to paragraph (3), it was generally found that, while the principle of contributory negligence might need to be borne in mind when preparing a revised version of draft article H, the specific provision contained in paragraph (3) might no longer be necessary, in view of the decision of the Working Group that the liability regime applicable to certification authorities should not be based only on negligence. With respect to paragraph (4), it was decided that the words "sustained by the user" should be deleted to extend the scope of the provision to losses sustained by any interested party.

73. After discussion, the Working Group requested the Secretariat to prepare a revised draft of article H, taking into account the above deliberations and decisions.

3. Issues of cross-border certification

74. The Working Group based its discussion of the issues of cross-border certification on the following draft provision:

"Draft article I

"(1) Certificates issued by foreign certification authorities may be used for digital signatures on the same terms as digital signatures subject to [this Law][these Rules] if they are recognized by an authorized certification authority, and the authorized certification authority guarantees, to the same extent as its own certificates, the correctness of the details of the certificate as well as the certificate being valid and in force.

"(2) The ... [the enacting State specifies the organ or authority competent to establish rules in connection with the approval of foreign certificates] is authorized to approve foreign certificates and to lay down specific rules for such approval."

75. Prior to beginning its deliberations on issues of cross-border certification, the Working Group was reminded that, under the mandate it received from the Commission, the Working Group was expected to advise the Commission as to the desirability and feasibility of preparing uniform rules on digital signatures, certification authorities and related issues (see above, para. 9). That mandate did not require the Working Group, at the current juncture, to finalize a draft text for consideration by the Commission at its thirtieth session.

76. The Working Group was also reminded of its previous discussions concerning the role of certification authorities within the framework of draft article B, particularly the differing views that had been expressed as to whether certification authorities would need to obtain a governmental approval to operate (see above paras. 40-50). The Working Group generally felt that it should be able to advance its deliberations on that issue after having considered issues of liability of certification authorities and cross-border certification. At the same time, it was noted that a decision on the issues raised by draft article B would also have implications for the regime of cross-border certification contemplated in the draft uniform rules.

77. As a general remark, the view was expressed that paragraphs (1) and (2) addressed the relationship between certificates issued by domestic certification authorities and foreign certificates from somewhat different angles. Paragraph (1) enabled a domestic certification authority to guarantee, to the same extent as its own certificates, the correctness of the details of the foreign certificate, and to guarantee that the foreign certificate was valid and in force. Under paragraph (2), the organ or authority competent for authorizing certification authorities in the enacting State was given the possibility of recognizing certificates issued by foreign certification authorities under the conditions it stipulated. It was suggested that the matters dealt with in paragraph (1) could be referred to as "cross-certification", while paragraph (2) dealt with a situation that would more accurately be referred to as "cross-border recognition". Those different issues might be better addressed separately.

78. The view was expressed that paragraphs (1) and (2) contained two different options for a possible regime of foreign certificates under the draft uniform rules. Support was expressed in

favour of each of the two options. It was widely felt, however, that those two options should not necessarily be regarded as mutually exclusive. While support was expressed in favour of placing the substance of paragraphs (1) and (2) under two separate articles, it was suggested that their respective spheres of application deserved further consideration. It was stated that paragraph (1) essentially contained a provision on the allocation of liability to the domestic certification authority in the event that the foreign certificate was found to be defective, a liability to be derived from draft article H. Paragraph (2), in turn, was not concerned with liability issues, but with the legal effects that might be produced directly by a foreign certificate, for example where that foreign certificate would be relied upon in the context of a dispute before the courts of the enacting State. Those legal effects were not necessarily predicated upon, or affected by, the existence of the guarantee contemplated in paragraph (1).

79. In view of the decision made by the Working Group to deal in the draft uniform rules not only with certification authorities licensed by public entities but also with "market-driven certification authorities" (see above, paras. 48-50), it was widely felt that draft article I should deal with the recognition of foreign certificates issued by both types of certification authorities.

80. It was suggested that the Working Group should also consider the question of the conditions under which foreign certificates could be recognized. Such conditions could take the form of governmental requirements, or be provided in arrangements between domestic and foreign certification authorities. Explanations were provided as to conceivable ways in which such arrangements between certification authorities might be structured. It was recalled that a public-key infrastructure was often based on various hierarchical levels of authority. Within those hierarchical structures, two stages of cross-certification seemed likely to occur. At an initial stage it was expected that cross-certification would be reserved exclusively to the "root authorities" (i.e., those authorities that certified the technology and practices in connection with the use of key pairs and registered subordinate certification authorities). At a later stage, as the industry developed, it was anticipated that also subordinate certification authorities placed below the "root" authority could become directly involved in guaranteeing the correctness of certificates issued by foreign certification authorities. In devising rules on issues of cross-certification, however, the Working Group should take into account the possibility that, particularly with respect to digital signatures involving the lowest degrees of security, foreign certificates might need to be enforced in the absence of a particular agreement between the certification authorities. It was therefore suggested that a default standard for recognizing foreign digital signatures issued in such circumstances might be needed.

81. It was stated that the inclusion of provisions dealing with issues of cross-border recognition might represent a significant step towards enhancing the trustworthiness of certificates. However, the methods and procedures for such cross-border certification or recognition had to be carefully considered by the Working Group. It was stated that, in assessing the trustworthiness of a foreign certificate, the recipient of a digitally signed message accompanied by the certificate should consider a number of questions, such as the following: whether the certification authority issuing the certificate was authorized to act abroad; whether the digital signature of the certification authority was authentic; whether legal recourse was available against the certification authority; whether the digital signature had been recognized to produce legal effects; and whether the digital signature could be enforced against its author.

82. From that perspective, it was further stated that cross-certification could basically provide four different levels of trustworthiness. At the highest level, the domestic certification authority, upon request of the party relying on a foreign certificate, would guarantee the contents of that certificate on the basis of its declared knowledge of the procedures that had led to the issuance of the certificate, thus assuming full liability for any errors or other defects in the certificate. At the immediately lower level, the domestic certification authority would guarantee the content of a foreign certificate based on the information it had received as to the trustworthiness of the foreign certification authority. A lesser degree of trustworthiness would be reached where the domestic certification authority limited its commitment to guaranteeing the trustworthiness of the foreign certification authority without assuming any liability for the contents of the foreign certificate. At the lowest level, the domestic certification authority would merely guarantee the identity of the foreign certification authority, based on a verification of its public-key and digital signature. It was suggested that the Working Group should pay attention to the level of comfort sought by the recipient of the message when formulating provisions on cross-certification or recognition of foreign certificates.

83. In that connection, a comparison was made between the position of a certification authority that guaranteed the correctness and the validity of a foreign certificate and that of a financial institution that guaranteed a letter of credit issued by a foreign bank. The acceptability of the letter of credit by its beneficiary was dependent upon factors such as the trustworthiness of the foreign bank issuing the letter of credit and the enforceability of that letter of credit in the country of the beneficiary. In some cases, the beneficiary might insist on obtaining a counter-guarantee from a local bank. The adequate level of security for the transactions would be established by the beneficiary of the letter of credit having regard to the level of risk the beneficiary was ready to assume. Similarly, a party to a transaction involving the use of a foreign certificate might be satisfied, for instance, with knowing that the certificate had been issued by a reputable foreign certification authority without deeming it necessary to obtain a guarantee from a domestic certification authority. The concern was expressed that draft article I might be perceived as discouraging or precluding the use of certificates that were not guaranteed by a domestic certification authority, even in the case of transactions where the parties felt reasonably confident with a lesser degree of security or legal certainty. It was important to ensure that draft article I dealt with the issues of cross-certification and cross-border recognition in a flexible manner.

84. In connection with the above comparison between the role of certification authorities and that of banks in the context of letter-of-credit transactions, it was generally felt that, in preparing uniform rules for the recognition of certificates, it should be borne in mind that digital signatures might be used not only for transferring rights but also for transferring obligations, for example where a digital signature was appended to a notice relating to an assignment of a debt. Therefore, the risk arising from reliance on a digital signature might need to be allocated to the recipient or to the issuer of the digital signature, depending on the type of transaction involved.

85. With regard to the possible scope of cross-certification and recognition, it was stated that, to a certain extent, functions performed by a certification authority resembled functions performed by a notary public under some legal systems. Indeed, in a number of legal systems certain types of transactions required that a notary public or another official performing similar functions certified

certain facts (e.g., the identity of one of the parties) or elements of the transaction (e.g., the signature of the parties or the authenticity of a document). However, the transactions for which such certification by a notary public were needed varied among different legal systems, and it would not be feasible to attempt to harmonize national solutions concerning formality requirements for the underlying transactions.

86. The view was expressed that the recognition of foreign certificates would often be provided on the basis of reciprocity, and therefore the authority for such recognition would be derived from bilateral or multilateral international agreements. Reservations were voiced to making reference to reciprocity in the draft uniform rules, given the varying meaning of "reciprocity" in different legal systems. The suggested addition of a reference to bilateral or multilateral international agreements, on the other hand, attracted varying reactions. In support of that suggestion, it was stated that making reference to bilateral or multilateral international agreements would make it clear that the draft uniform rules did not affect the international obligations that States might assume, for instance within the framework of regional agreements on economic integration or cooperation. However, it was also stated that no special reference to such agreements was needed, since nothing in paragraph (1) prevented the enacting State from achieving cross-certification or recognition of foreign certificates through such agreements. It was further suggested that, instead of referring to international agreements in draft article I, the Working Group should consider formulating substantive rules for the recognition of foreign certificates. It was said that a reference to bilateral or multilateral international agreements within the context of article I should be avoided unless: (a) the Working Group came to the conclusion that it was not feasible to establish harmonized rules of recognition; or (b) such a reference related to agreements that provided a more favourable level of recognition of foreign certificates than the one provided in the draft uniform rules.

87. It was stated that paragraphs (1) and (2) contained two different options available to the enacting State, depending on whether or not the operation of a certification authority required prior governmental approval. However, the concern was voiced that, when read in conjunction with draft article B, which required such prior approval for certification authorities established in the enacting State, paragraph (1) might be read as allowing the recognition of certificates issued by foreign certification authorities which had not been authorized to operate under domestic rules, while denying legal effectiveness to certificates issued by domestic certification authorities that had not received the required authorization in the enacting State. In that connection, a question was raised as to whether the purpose of draft article I was to make it possible for a governmentally-authorized certification authority to extend legal value to certificates issued by other, unauthorized certification authorities, domestic or foreign. If that was its intended purpose, draft article I might need to be revised in the light of the decision to be made by the Working Group with respect to draft article B.

88. In respect of the guarantee provided under paragraph (1), it was stated that some legal systems might have difficulties in dealing with that issue by way of a general provision, without adding more detailed provisions in view of the fact that warranties provided by certification authorities might vary greatly in different countries. If would be difficult for domestic certification authorities to assume liability for certificates issued abroad without a common ground concerning the types of warranties offered by certification authorities.

89. After considering the different views expressed in the Working Group, it was generally felt

that it was appropriate to deal with the issues of cross-border certification in the draft uniform rules. While the principles reflected in draft article I were regarded as broadly acceptable, it would be premature for the Working Group to attempt to formulate detailed provisions on those issues at such an early stage in its deliberations. The Secretariat was requested to prepare a revised draft of article I, taking into account the above deliberations, and based on the need to accommodate both publicly-licensed and non-licensed certification authorities. The Secretariat was requested to distinguish between the conditions and effects of recognition of a digital signature and a certificate, on the one hand, and the recognition of a certification authority on the other hand, and to make appropriate proposals, possibly in the form of variants, for dealing with those different issues.

1. Definitions (continued)

(b) Authorized certification authorities (continued)

90. Having completed its preliminary consideration of the issues of liability and cross-certification under draft articles H and I, the Working Group resumed its deliberations on the issues raised by the definition of "certification authority" under draft article B (see above, paras. 40-49). It was recalled that, in order to accommodate both the situation where certification authorities operated on a purely private basis and the situation where certification authorities should be licensed or otherwise authorized by public authorities before they were allowed to operate, the Working Group had decided, tentatively, to adopt a "dual approach" (see above, paras. 48-50), which suggested the need for a broad definition of "certification authority" to cover both types of situations. In that connection, it was suggested that the Working Group might give consideration to the possibility of replacing the notion of "certification authority" by that of "certification entity", to avoid the possible implication that functions of certification were necessarily performed by public authorities. While support was expressed in favour of that suggestion, it was recalled that the notion of "certification authority" was already used widely, by both public and private entities. The Working Group was urged to exert caution in adopting terminology that might contradict emerging certification practice.

91. It was pointed out that the provisions currently embodied by draft article B addressed various aspects of certification authorities. While certain paragraphs, such as paragraph (3), were of a purely definitional nature, other provisions, such as paragraph (4), were more operational and descriptive of the functions performed by certification authorities. It was thus suggested that draft article B might need to be subdivided into different articles, dealing with the definition and the functions of certification authorities, respectively. It was widely felt that, in restructuring draft article B, it might be appropriate to refer to functions that might be performed by certification authorities in addition to time-stamping, such as the issuance of key pairs, maintenance of directories, retention of records and other services, which were described as "ancillary" to the main functions performed by certification authorities with respect to digital signatures. It was generally agreed, however, that the effect of addressing such ancillary services should not be to expand the scope of the uniform rules, as defined by reference to "digital signatures" in draft article A.

92. As a possible distinction between the legal regimes applicable to certification authorities licensed or otherwise authorized by the enacting State, and to non-authorized certification authorities, it was suggested that the draft uniform rules should spell out the specific legal effects

that might be expected from the issuance of certificates by authorized certification authorities. In response to a question that was raised as to the legal effects that might flow from the issuance of certificates by non-authorized certification authorities, it was suggested that the matter might be dealt with by way of a mere reference to article 7 of the Model Law. While support was expressed in favour of that proposal, it was stated that it might be appropriate for the uniform rules to elaborate on the legal effects achieved by certificates that emanated from purely private certification authorities. Another suggestion was that a possible distinction between authorized and non-authorized authorities might be based on different functions that might be performed by the two types of authorities. It was generally felt that those issues might deserve further consideration by the Working Group at a future session.

93. In the context of the discussion of paragraph (3), a question was raised as to whether the reference to "keys of natural and legal persons" provided sufficient guidance in situations where cryptographic keys were issued directly to electronic devices, or used by such devices, in the absence of direct human intervention. The Working Group recalled that the issue had been discussed in the context of the preparation of the Model Law, and generally agreed that it might need to be discussed further at a later stage in connection with the issues of digital signatures.

94. As to the possible structure of a revised draft of article B, the attention of the Working Group was drawn to the method followed with respect to the Model Law, which relied on a combination of statutory provisions with a guide to enactment of such provisions. Adopting that method made it possible to include more detailed explanations and illustrations as to the contents of the statutory provisions, thus facilitating their future consideration by legislators. It was suggested that the same approach should be taken with respect to the uniform rules. Particularly in dealing with the various functions performed by certification authorities, it would be appropriate to include explanatory material in the context of a guide to enactment. The Working Group, while postponing its decision as to the final form of the uniform rules, found that suggestion to be generally acceptable as a working assumption.

95. After discussion, the Working Group decided that the provisions currently found in draft article B should be relocated in two separate articles, dealing with an expanded definition of "certification authority", and with the functions performed by certification authorities, respectively. It was decided that the general definition of "certification authority" should be based on the text of paragraph (3) of draft article B. It was agreed that the reference to "natural and legal persons" should be complemented by a reference to "electronic devices", which should be placed between square brackets, pending future consideration by the Working Group. In addition to a general definition of "certification authority", the revised definitional article should contain a definition of "licensed", "authorized" or "accredited" certification authorities, which could be based on paragraph (1) of draft article B. As to the elements contained in paragraphs (2) and (5) of the draft article, they should be reflected in the portion of the guide to enactment of the draft uniform rules corresponding to the definition of "authorized" certification authorities.

96. It was generally agreed that the separate article, which should deal with the various functions provided by certification authorities, could be based on paragraph (4) of draft article B. It was also agreed that the scope of a future article on functions of certification authorities might appropriately be expanded to cover other functions. To that effect, elements might be drawn from existing pieces

of legislation, guidelines and model contracts in use or being considered for adoption with respect to certification authorities. As a matter of drafting, it was generally felt that the reference to "communication secured by means of digital signatures" in paragraph (4) might need to be amended to avoid suggesting particular implications as to the acceptability of security methods used by certification authorities.

97. The Secretariat was requested to prepare a revised draft of article B, taking into account the above deliberations and decisions.

(c) Certificates

98. The Working Group based its discussion of the definition of certificates on the following draft provision:

"Draft article C

"The certificate issued by an authorized certification authority, in the form of a data message or otherwise, shall indicate at least:

"(a) the user's name [and address or place of business];

"(b) [the day and year of birth][sufficient identification] of the user if the user is a natural person;

"(c) if the user is a legal person, the name of the company and any relevant information for identifying that company;

"(d) the name, address or place of business of the certification authority;

"(e) the user's public cryptographic key;

"(f) any necessary information indicating how verification of the user's public cryptographic key is available to the recipient of the digital signature given according to the certificate;

"(g) the serial number of the certificate; and

"(h) the [date of issuance and the date of expiry][validity period] of the certificate."

99. At the outset, the Working Group was reminded that, during its deliberations on the definition of "certification authority", the Working Group had agreed, as a working assumption, to adopt a flexible approach that covered certificates issued by both governmentally-authorized certification authorities and certification authorities functioning outside a governmentally- implemented public-key infrastructure, without at the current stage excluding either of those alternatives.

Consistent with that working assumption, the word "authorized" in the chapeau of draft article C should be deleted.

100. General remarks were made concerning the terminology of draft article C, in particular the use of the word "user" with reference to the holder of the private key of a cryptographic key pair. That word was felt to lend itself to confusion with the recipient of a message, who could be regarded as being the "user" of the certificate or of the public key used for verifying the digital signature. A number of alternatives were suggested, including the expressions "owner of the key pair", "holder of the certificate", "holder of the private key". It was agreed that the Secretariat should review the terminology used in draft article C and in the remaining provisions of the draft uniform rules and formulate proposals for avoiding possible ambiguities.

101. It was widely felt that draft article C should define "certificate" prior to mentioning its required content. One proposed definition was along the following lines: "A certificate is a data message that purports to be a certificate, identifies the certification authority, contains the public key of the user, names the user and is digitally signed by the certification authority." Another proposal was that a definition should be based on the elements of a certificate contained in the note by the Secretariat, which referred to the certificate as being an electronic record that listed a public key together with the name of the certificate subscriber as the "subject" of the certificate, and confirmed that the prospective signer identified in the certificate held the corresponding private key (A/CN.9/WG.IV/WP.71, para. 36). It was felt that a definition such as that suggested in the latter proposal would be generally acceptable. However, such a definition should specify that, if the certificate was delivered by electronic communication, the certification authority should digitally sign it to assure the authenticity of the certificate with respect to both its contents and source.

102. A question was raised as to whether the words "at least" in the chapeau of draft article C in connection with the content of a certificate meant that a certificate which did not contain all the information and data listed in draft article C would not be regarded as a certificate within the meaning of the draft uniform rules. In reply, it was stated that, as currently drafted, the draft article mentioned a number of mandatory elements that had to be contained in a certificate in order for it to be regarded as such under the draft uniform rules. For clarity purposes, it was suggested that the definition of "certificate" should be a self-contained provision and that the information required to be provided in a certificate should be listed in a separate provision.

103. The Working Group discussed the level of information that should be contained in a certificate. As a general remark, it was suggested that the mandatory elements should be kept to a minimum and should include essentially the information that was required in order for the user of the certificate to be able to verify the digital signature used in a data message. The concern was expressed that the inclusion of unnecessary elements among the information to be contained in a certificate might inadvertently exclude from the ambit of the draft uniform rules a number of certificates which might otherwise be sufficient for the purposes for which they had been issued. The view was expressed that it was important to bear in mind the difference between the information contained in a certificate and the steps that had to be taken by the certification authority to establish the accuracy of that information. The more information was contained in a certificate, the greater the risk was that liability might be incurred by the certification authority. Accordingly, it was suggested that no minimum requirements should be established by the draft uniform rules as to the

contents of a certificate.

104. A different approach was suggested, based on the discussion of the issue of liability of certification authorities, in the context of which it had been understood that, in the event of erroneous identification of a person or erroneous attribution of a public key to a person, the certification authority would be held liable for the loss sustained by any injured party unless the certification authority could demonstrate that it had exerted its best efforts to avoid the error (see above, para. 58). It was generally felt that it would be of little avail for the purpose of protecting the end-users to require the certification authority to follow adequate procedures for establishing the accuracy of the information, or properly identifying the holders of private keys, and at the same time to allow the certification authority to avoid liability by issuing certificates that fell below the minimum level of information required to be contained in a certificate.

105. It was suggested that, if the certificate had to meet a certain number of mandatory requirements as to its contents, a certification authority would not be free to avoid liability in the manner that had been alluded to. In that connection, it was recalled that in the discussion of the issue of liability of certification authorities, a proposal had been made that any certification authority, when issuing a certificate, should be under an obligation to represent that it had confirmed a number of elements (see above para. 70). Strong support was expressed in favour of that suggestion. After discussion, the Working Group agreed that the matter could not be examined thoroughly at the current session. It was agreed that deliberations on the subject would need to be resumed at the earliest possible opportunity, on the basis of variants to be prepared by the Secretariat to reflect the above discussion.

106. With regard, in particular, to data that might be required for identifying the holder of the private key, it was suggested that subparagraphs (a), (b) and (c) should be combined into one single provision. In that connection it was noted that in many countries information regarding, for example, the date of birth of a person was protected as personal data, and specific rules might govern its disclosure by electronic means. Therefore, it was suggested that personal information of that kind should not be required to be contained in a certificate. In reply it was stated that in certain circumstances a person making an application for a certificate might consent to, or have an interest in, the release of certain types of personal data or sources of additional information. The draft uniform rules should not preclude such a possibility in cases where the consensual release of personal data would not conflict with applicable rules on data protection or the public policy of the State where such application was made or the certificate was issued. It was generally felt that questions concerning data protection fell outside the scope of the draft uniform rules and that draft article C should require only that sufficient identification be provided consistent with applicable laws on data protection.

107. It was suggested that subparagraph (a) should refer to the user's "name or identification", so as to encompass situations in which the user would not be identified by its name but rather by other means of identification such as an account number, as could be the case of certificates relating to credit card transactions. That suggestion was objected to on the ground that it might encourage the use of anonymous messages and certificates, a situation which would not be in keeping with the objective of promoting greater legal certainty in electronic commerce. The Working Group was urged to retain reference to the name of the holder of the private key as an essential element of a

certificate.

108. For the purpose of ensuring proper identification of the holder of the private key, it was suggested that draft article C should retain a reference to additional elements of identification such as the address, in the case of natural persons, or the registration number, in the case of legal entities, since the name of a person or company might not in itself be sufficient for identifying that person or company.

109. The view was expressed that the use of a digital signature might in some cases be restricted to certain types of transactions, for example as a result of limitations on the authority of the signor to bind the company in the name of which the transaction was made. It was thus suggested that the certificate should contain information on such restrictions or limitations, or should make reference to their source. In reply to that suggestion it was noted that the question of the limits within which a digital signature might be relied upon raised a number of difficult legal issues, which were not unique to electronic commerce. In a paper-based environment it might not be mandatory for a handwritten signature to be accompanied by a declaration on the limitations, if any, of the powers of its author. The Working Group was urged not to introduce, in connection with digital signatures, requirements more stringent than those that applied to handwritten signatures.

110. The Working Group was reminded of its earlier discussion concerning consumer issues and the liability of a certification authority and the possible limitations or exclusions of liability pursuant to national law or the certification authority's certification practice statement. It was suggested that the certification authority should be required to state such limitations or to make reference to a document accessible to the user, where such limitations could be found. It was also suggested that the draft uniform rules should provide the consequences that would flow from the absence of such indication in the certificate. Similarly, it was suggested that, where the validity period of a certificate was limited, such limitations should be mentioned in the certificate, in the form of an expiry date or an operational period. It was felt that it was important for the protection of users of certificates that they should be provided with information as to the validity of certificates and that they should not bear the risk that a certificate might be issued without such indication. Therefore, the draft uniform rules should contain a default provision specifying the validity period that would apply in the absence of such indication. However, it was pointed out that the existence of such a rule should be interpreted as meaning that the certification authority had the option to omit mentioning the validity or operation period of a certificate.

111. Questions were raised as to the type of information that certification authorities were able to provide the users of their services in accessible form taking into account the technology currently available. In response, it was stated that existing technology allowed the certification authorities to append or otherwise link to the certificates they issued additional information, such as their own certification practice statement or information optionally made available for that purpose by the holders of private keys. However, many computer systems currently in use by the customers of certification authorities were still incapable of accessing all such information. Besides such technical difficulties, it was important to bear in mind that some of the information that might be appended to certificates might originate from the holders of private keys and be released pursuant to their request. It was important in those cases to distinguish between elements of the certificate which were certified by the certification authority (e.g., identity of the private-key holder) from others

provided by their customers and not verified by the certification authorities (e.g., limitations on the use of private keys within a corporation). The certification authorities should not be made liable for the accuracy of such non-verified information.

112. Various interventions were made to the effect that, without prejudice to other possible information that certification authorities might provide to their customers, they should represent and warrant that the accuracy and completeness of the information which was mandatorily to be contained in a certificate had been verified.

113. After considering the views expressed in connection with draft article C, the Working Group agreed that a definition of "certificate" should be added to the draft article. The mandatory content of the certificate should be provided in a separate provision, which should also deal with the consequences of the absence of mandatory elements of a certificate. That provision should reflect the elements referred to in subparagraphs (a), (b) and (c), combined into one single revised provision, and include also the information mentioned in subparagraphs (d), (e) and (h) of draft article C. The information referred to in subparagraph (f) was not considered capable of being certified by a certification authority and, accordingly, it was agreed to delete the subparagraph. It was agreed that subparagraph (g) should be placed within square brackets and considered at a later stage as a possible option, since not all certificates might be identified by way of a serial number. The revised draft of article C should make express reference to the applicability of domestic law on data protection to the information to be contained in a certificate. The Secretariat was requested to prepare a revised draft of article C reflecting, as possible variants, the various views expressed and the conclusions reached by the Working Group.

4. Signature by legal and natural persons

114. The Working Group based its discussion on the following draft provision:

"Draft article D

"(1) Natural and legal persons may equally obtain certification of cryptographic public keys used exclusively for identification purposes.

"(2) A legal person may identify a data message by affixing to that message the public cryptographic key certified for that legal person. The legal person shall only be regarded as [the originator][having approved the sending] of the message if the message is also digitally signed by the natural person authorized to act on behalf of that legal person."

115. A number of delegations expressed the view that that draft article D should be deleted. It was stated that distinguishing between legal and natural persons for the purposes of digital signatures was inappropriate in view of the fact that no such distinction was made in the Model Law, where the notion of "person" covered both natural and legal persons. Moreover, it was stated that paragraph (2) might inappropriately interfere with other bodies of law, e.g., agency law, and with the provisions of company law dealing with representation of companies by natural persons.

Furthermore, it was stated that the rule contained in paragraph (2) appeared to impose on users of digital signatures a burden that went beyond existing requirements with respect to handwritten signatures.

116. The view was expressed, however, that draft article D, and more specifically paragraph (2), served a useful purpose. In particular, where no other applicable rule of law specified the form in which a binding signature might be given on behalf of a legal person, a default rule along the lines of paragraph (2) might provide useful guidance as to the circumstances under which a digital signature purported to be that of a legal person might be relied upon. Support was expressed in favour of retaining paragraph (2), provided that the provision was redrafted to indicate clearly that, although it contained a reference to "a natural person authorized to act on behalf" of a legal person, it was not intended to displace the domestic law of agency. The question as to whether the natural person did in fact and in law have the authority to act on behalf of the legal person would thus be left to the appropriate legal rules outside the uniform rules.

117. After discussion, the Working Group decided that draft article D should be placed between square brackets, for further consideration at a later session.

5. Attribution of digitally-signed messages

118. The Working Group based its discussion on the following draft provision:

"Draft article E

"(1) The originator of a data message on which the originator's digital signature is affixed is bound by the content of the message in the same manner as if the message had existed in a [manually] signed form in accordance with the law applicable to the content of the message.

"(2) The addressee of a data message on which a digital signature is affixed is entitled to regard the data message as being that of the originator, and to act on that assumption, if:

"(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied the originator's public key to the data message as received and the application of the originator's public key revealed: that the received data message had been encrypted with the originator's private cryptographic key; and that the initial message had not been altered after being encrypted through the use of the originator's public cryptographic key;

"or

"(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to the originator's private cryptographic key.

"(3) Paragraph (2) does not apply:

"(a) as of the time when the addressee knew or should have known, had it sought information from the authorized certification authority or otherwise exercised reasonable care, that the validity of the originator's public cryptographic key had expired, or that the certificate issued by the certification authority had been revoked or suspended;

"or

"(b) in a case within paragraph (2) (b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator."

119. The view was expressed that draft article E should be deleted. In support of that view, it was stated that the draft article merely provided an industry-specific version of article 13 of the Model Law and might create uncertainty as to the possible interplay of the two provisions. Another view was that the draft article should be deleted because it might be misinterpreted as interfering with the law applicable to the commercial transaction for the purpose of which a digital signature was used. For example, the provisions of paragraph (1), under which the originator of a data message was "bound by the content of the message", might be read as inappropriately dealing with general contract law.

120. The prevailing view was that, while the specific drafting of draft article E might need to be modified, the principle contained in paragraph (1) was useful in establishing the legal consequence of using a digital signature. As to how such a principle might be expressed, a suggestion was made that paragraph (1) should be redrafted in the form of an irrebuttable presumption to the effect that the holder of a digital signature would be deemed to be the signer of a data message to which that digital signature was affixed.

121. With respect to the possibility that the issue of attribution of digitally-signed messages might be dealt with by way of presumptions, whether rebuttable or not, it was suggested that further distinctions might need to be made according to the kind of transaction for which digital signatures might be used. For example, the same standard should not be used for purely commercial transactions between long-term trading partners and for the submission of tax declarations to public administrations.

122. It was suggested that a provision along the lines of paragraph (1) might need to distinguish between different kinds of digital signatures (e.g., the various levels of security performed by various algorithms, and the corresponding variation in the costs of digital signatures) and different circumstances under which digital signatures were used. It was suggested that, in preparing a revised draft of paragraph (1), the following categories might be taken into account: whether a digital signature was used outside any pre-existing contract between the parties; whether a digital signature was used in the context of a contractual framework; whether a digital signature involved the issuance of a certificate by a non-accredited certification authority; or whether a certificate was issued by a licensed certification authority. It was also suggested that, in dealing with the various

levels of risk involved in the digital signature process in case of fraud, particular attention should be given to the situation where fraud occurred prior to the issuance of a key pair. In such a situation, in the absence of any agreement between the parties, the burden of establishing the link between the digital signature and the sender should be borne by the recipient. If a certificate was issued, and the certificate was appropriate and valid, the burden of proof might be shifted. Another suggestion was that, in dealing with messages certified by a certification authority, the party that designated a given certification authority should bear the risk involved by the use of the certificates issued by that certification authority.

123. Doubts were expressed as to whether all of the above-mentioned categories should be taken into account in revising draft article E. It was recalled, in particular, that in the context of its discussion of liability issues, the Working Group had agreed to focus on situations where a certificate was issued. It was generally felt, however, that some or all of the suggested categories should be borne in mind when preparing a revised draft of article E for consideration by the Working Group at a future session.

124. After discussion, the Working Group agreed that a revised provision on attribution of digitally-signed messages was necessary for further consideration by the Working Group and that such a provision might be developed along the lines of paragraph (1) of draft article E. It was generally felt that appropriate comments might be needed to clarify the relationship between article E and articles 7 and 13 of the Model Law. The Secretariat was requested to prepare a revised draft of article E, with possible variants reflecting the above discussion.

6. Revocation of certificates

125. The Working Group based its discussion concerning revocation of certificates on the following draft provision:

> "Draft article F
>
> "(1) The holder of a certified key pair may revoke the corresponding certificate. The revocation is effective from the time when it is [registered] [received] by the certification authority.
>
> "(2) The holder of a certified key pair is under an obligation to revoke the corresponding certificate where the holder learns that the private cryptographic key has been lost, compromised or is in danger of being misused in other respects. If the holder fails to revoke the certificate in such a situation, the holder is liable for any loss sustained by third parties having relied on the content of messages as a result of the holder's failure to undertake such revocation."

Paragraph (1)

126. General remarks were made as to the meaning of paragraph (1). It was stated that the holder of the private key should always have the right to request the certification authority to revoke a certificate. The fact that such a revocation became effective upon receipt or registration by the certification authority should not be interpreted as a limitation to that right. Also, the fact that such a revocation became effective upon receipt or registration by the certification authority should not be interpreted to the effect that the third parties had the duty to ascertain the validity of a certificate (e.g., that the certificate had not been revoked) prior to relying on a certificate, a proposition which raised a number of objections in the Working Group (see above, para. 60).

127. Various views were expressed as to the time from which such a revocation was effective. Under one view, the revocation should be effective from the time it was registered by the certification authority, since the time of receipt might in some cases be difficult to establish, thus leading to uncertainties as to the point in time when a certificate ceased to be valid. Under another view, the certification authority should have the obligation to act promptly upon the revocation of a certificate so as to avoid any loss that might be sustained by the holder of the private key or third parties, and that might result, for instance, from a certificate being inadvertently accepted after such a certificate had been repudiated by its holder. Therefore, the effects of the revocation of a certificate should be dependent upon measures to be taken by the certification authority over which the holder of the private key had no control.

128. Questions were raised as to the possible effect of the registration of revocation of a certificate. In that connection, the view was expressed that the notion of registration of the revocation of a certificate might not be entirely adequate for the purposes intended by draft article F, which aimed, inter alia, at ensuring that third parties were apprised, as appropriate, of the fact that a particular certificate had been revoked. It was stated that, upon receipt of a request concerning the revocation, a certification authority might in some cases have to verify the authenticity of such request, a procedure which, depending upon the circumstances, might entail some delay. The appropriate moment for such revocation to become fully effective, therefore, was the time it was released to the general public by being placed in a generally accessible database maintained by the certification authority, or by other appropriate publication method.

129. In view of the latter comments, it was stated that the receipt of the request for revocation was still preferable to the registration for the purpose of establishing the time from which the certificate was regarded as having being revoked. However, if the notion of receipt of such requests was not to be found sufficiently precise, the receipt could be combined with some action to be subsequently taken by the certification authority to effect such revocation, such as publicizing the revocation or issuing notice thereof.

130. In order to advance its deliberations on the subject, the Working Group was invited to consider the general implications of a choice regarding the time in which the revocation became effective, as well as the parties that might be affected by such revocation. The moment in which the revocation became effective would be crucial for determining the respective liabilities of the holder of the private key and the certification authorities as between themselves and vis-à-vis third parties. It was suggested that it might be advisable for the Working Group to consider dealing with each of those situations separately. In support of that proposal, it was pointed out that each of the alternatives currently contained in paragraph (1) had its own merits. As between the holder of the

private key and the certification authority, it might be appropriate to provide that the revocation should become effective upon receipt by the certification authority of the request for revocation made by the holder of the private key. Vis-à-vis third parties, however, it might be more appropriate to require prior registration or publication in order for the notice to become effective.

131. It was pointed out that the effective time of the revocation had significant consequences for the liability of the certification authority and that both issues should be addressed in an harmonious manner. It was noted that draft article H, paragraph (4), provided that, where an authorized certification authority had received notice of revocation of a certificate, the authority should register such revocation forthwith. If the certification authority failed to do so, it should be liable for any resulting loss sustained by the user. Thus, if the draft uniform rules provided that revocation of a certificate became effective at the time when it was received, paragraph (4) of draft article H should be deleted since there could be no basis for the liability of the certification authority for fault or negligence in the registration of the revocation. However, if the revocation of a certificate was to become effective at the time when it was registered, there might be no need for a provision other than article H, paragraph (4).

132. In response to that comment it was stated that the rule contained in draft article H, paragraph (4), should be retained, irrespective of the choice of the Working Group concerning the two alternatives currently provided in article F, paragraph (1). Late registration of a request for revocation might be the cause of some loss, either to the owner or to the relying party, and therefore a rule on liability for the consequences of late registration would still be needed.

133. In that connection, it was stated that international standards and guidelines on electronic certification and authentication, such as the Uniform International Authentication and Certification Practice Guidelines being prepared by the International Chamber of Commerce, reflected the principle that a certification authority had to act promptly on a request for revocation of a certificate. However, as had been previously noted, there might be some delay in giving effect to such a request, particularly where, under the circumstances, the certification authority needed to conduct some verification, such as to confirm the authority of the persons who requested the revocation on behalf of the holder of the private key. In order to avoid an inadvertent use of the certificate during the period where a request for its revocation was being verified by a certification authority, it was suggested to include in the draft uniform rules a provision whereby a certification authority should suspend a certificate promptly upon request of a holder of a private key. It was explained that, unlike the revocation, which terminated the validity of the certificate, the suspension was a temporary measure that only withheld the validity of the certificate for a certain period.

134. Support was expressed for introducing the notion of suspension of a certificate, as distinct from its outright revocation. However, it was suggested that such suspension should be dealt with in a separate provision, since the notion and effects of a suspension were different from those of a revocation.

135. After having considered the different views expressed, the Working Group agreed that the issue of revocation of certificates was an important part of an adequate legal regime of digital signatures and deserved further consideration by the Working Group. It was generally felt that additional elements were needed in a provision dealing with the subject, and the Secretariat was

requested to prepare a revised provision taking into account the deliberations of the Working Group and including possible variants dealing with the time from which a revocation became effective. It was also agreed that the revised draft should contain provisions on the suspension of a certificate.

Paragraph (2)

136. It was suggested that the use of the word "obligation" in the first sentence of the paragraph was not entirely appropriate and that it would be preferable in that context to use other words such as "onus" or "duty".

137. The suggestion was made that, in addition to the holder of a certified key pair, the certification authority, too, should have the duty to revoke the corresponding certificate where the certification authority learned that the private cryptographic key had been lost, compromised or was in danger of being misused in other respects. In support of that suggestion it was stated that some international standards and guidelines on electronic certification and authentication, such as the Uniform International Authentication and Certification Practice Guidelines being prepared by the International Chamber of Commerce, contemplated such a duty.

138. In response to questions concerning a certification authority's ability to fulfil such a duty, it was stated that the currently available technology allowed a certification authority to respond quickly in those situations. However, the time needed for such a response was not only a function of the technology available, but depended also on the level of service provided by a certification authority to its customers under the terms of their contractual arrangements (e.g., whether the certification authority had designated staff to deal with loss, compromise or misuse of private keys; whether the certification authority offered customer services during weekends or only during ordinary office hours).

139. The Working Group took note of the views expressed and agreed that they should be taken into consideration in its future deliberations on the issue of revocation of certificates.

7. Register of certificates

140. The Working Group based its discussion on register of certificates on the following draft provision:

"Draft article G

"(1) An authorized certification authority shall keep a publicly accessible electronic register of certificates issued, indicating when the individual certificate was issued, when it expires or when it was suspended or revoked.

"(2) The register shall be maintained by the certification authority for at least [10] years after the date of revocation or expiry of the operational period of any certificate issued by that certification authority."

141. The Working Group was invited to begin its discussion on register of certificates by considering the importance of including a provision on that issue in the draft uniform rules and, in the event of a positive answer to that question, by considering the elements of such register and the retention period, if any, that should be provided.

142. While no objections of principle were raised to including a provision on register of certificates, it was suggested that the Working Group should keep under consideration the question whether such a provision was in fact necessary in the context of the draft uniform rules or was relevant for all the different types of certificates that might be issued by certification authorities.

143. With respect to the manner in which such a register should be structured, the view was expressed that, instead of maintaining each its own register of certificates, certification authorities belonging to the same public-key infrastructure might benefit from maintaining a centralized registry in which they would lodge the certificates they issued. Such a structure, which would aim at avoiding multiple registries, was currently being considered in some countries. It was suggested that it might be useful for the Working Group to examine that possibility further.

144. As regards paragraph (1), it was suggested that it was not necessary to indicate the date of issuance of a certificate in the register and that, accordingly, the words "indicating when the individual certificate was issued" should be deleted. Another suggestion was that certification authorities should maintain a separate database of revocation of certificates in order to facilitate inquiries by interested parties concerning the validity of certificates.

145. Differing views were expressed as to the need for, and adequacy of, the retention period referred to in paragraph (2). It was stated that providing a minimum retention period was relevant for the purpose of ensuring the availability of data to interested parties, a measure which was of particular importance within the context of time-limits existing under national laws for exercising or enforcing rights or demanding the performance of obligations. However, national laws had different time-limits for different types of rights and obligations. Similarly, they provided different retention periods for public and private records according to their respective objects. In the circumstances, it might be preferable to leave it for national law to determine what would be an appropriate retention period, rather than arbitrarily establishing a period that might not be adequate in all circumstances. Furthermore, the Working Group should bear in mind the cost entailed in maintaining a register of certificates over any given period of time. Depending on the level of service provided by the certification authority and the method used for filing certificates, it might not be cost-effective for a certification authority to undertake to retain some types of certificates beyond a certain period of time. It would not be advisable to attempt to provide a general retention period without information on the practical implications of such a rule for the industry.

146. Another view, however, was that the question of the retention period of records and information that allowed an interested party to establish the identity of its trade partners and the authenticity of their signatures involved a number of public-policy considerations that should not be ignored by the Working Group. That question deserved to be addressed in the draft uniform rules. As to the appropriate retention period it was suggested that certification authorities should not be free to stipulate unilaterally the retention period solely on the basis of their cost considerations.

Furthermore, the cost of retention alone should not be a determinant factor for shortening or suppressing the retention period. Certification authorities that filed the certificates they issued with the same registry within a public-key infrastructure could establish some mechanism for sharing the cost among themselves.

147. A suggestion was made to the effect that interested parties making inquiries in a register of certificates should be required to leave in it a trace giving some evidence that such an inquiry had been made. It was explained that the existence of such evidence might be of importance in the event that questions arose between the certification authority and such interested party as to whether the interested party had verified the validity of a certificate prior to relying on a digitally-signed message.

148. The Working Group took note of the different views expressed and requested the Secretariat to review the issues raised and formulate alternative draft provisions reflecting the debate that took place within the Working Group.

8. Relations between users and the certification authority

149. The Working Group had before it the following draft provision:

"Draft article J

"(1) A certification authority is only allowed to request such information as is necessary to identify the user.

"(2) Upon request from legal or natural persons, the certification authority shall deliver information about the following:

"(a) the conditions under which the certificate may be used;

"(b) the conditions associated with the use of digital signatures;

"(c) the costs of using the services of the certification authority;

"(d) the policy or practices of the certification authority with respect to the use, storage and communication of personal information;

"(e) the technical requirements of the certification authority with respect to the user's communication equipment;

"(f) the conditions under which warnings are given to users by the certification authority in case of irregularities or faults in the functioning of the communication equipment;

"(g) any limitation of the liability of the certification authority;

"(h) any restrictions imposed by the certification authority on the use of the certificate;

"(i) the conditions under which the user is entitled to place restrictions on the use of the certificate.

"(3) The information listed in paragraph (1) shall be delivered to the user before a final agreement of certification is concluded. [That information may be delivered by the certification authority by way of a certification practice statement.]

"(4) Subject to a [one-month] notice, the user may terminate the agreement for connection to the certification authority. Such notice of termination takes effect when received by the certification authority.

"(5) Subject to a [three-month] notice, the certification authority may terminate the agreement for connection to the certification authority. Such notice of termination takes effect when received."

150. The Working Group noted that, to the extent that draft article J dealt with the relations between users and certification authorities, it presupposed decisions on a number of issues which were still under consideration by the Working Group. It was agreed that the entire draft article J should be placed in square brackets and should be considered by the Working Group at a later stage.

III. INCORPORATION BY REFERENCE

151. Having completed its preliminary consideration of the legal issues and possible provisions to be considered in uniform rules on digital signatures, as reflected in part II of the present report, the Working Group noted that, for lack of sufficient time, it could not enter into any detailed discussion of the issues of incorporation by reference at the current session.

152. The Working Group recalled that the issue of incorporation by reference had been briefly discussed at various stages during the preparation of the Model Law (see A/CN.9/406, paras. 90 and 178, and A/CN.9/407, paras. 100-105 and 117). At its previous session, the Working Group was generally agreed that work was needed with respect to incorporation by reference in the context of electronic commerce. The view was expressed that, in any attempt to establish legal norms for such incorporation of reference clauses in data messages, the following three conditions should be met: (a) the reference clause should be inserted in the data message; (b) the document being referred to, e.g., general terms and conditions, had actually to be known to the party against whom the reference document might be relied upon; and (c) the reference document had to be accepted, in addition to being known, by that party. It was generally agreed that the topic of incorporation by reference would appropriately be dealt with in the context of general work on the issues of registries and service providers (A/CN.9/421, para. 114). The Commission, at its twenty-ninth session, was generally agreed that the issue could be dealt with in the context of work on certification authorities.

2/

153. At the current session, there was general agreement that the acceptability of incorporation by reference was of considerable importance for the development of electronic commerce in general. While that issue might need to be discussed in the context of work on digital signatures and certification authorities, it would also deserve consideration at a more general level. Even if it was later found appropriate to devise specific rules for incorporation by reference in the context of digital signatures, a general discussion and possibly a general set of rules were needed.

154. The view was expressed that devising rules for incorporation by reference in an electronic environment might be a difficult task, in view of the complexity of the issues involved. Incorporation by reference and related issues, such as adhesion contracts and "battle-of-forms" issues, had given rise to a wide variety of legal rules in a paper-based environment, and not all the related legal issues had been solved satisfactorily. The topic made it necessary to balance conflicting interests. On the one hand, there existed a need to recognize party autonomy. On the other hand, possible abuses of adhesion contracts should be limited. In view of the difficulties expected to be met in the area of incorporation by reference, it was suggested that higher priority should be given to other issues that might also warrant further work in the context of electronic commerce. Another view was that a discussion of incorporation by reference could only be engaged on the basis of further studies by the Secretariat with respect to the comparative law aspects of adhesion contracts, battle-of-forms and related liability issues.

155. The widely prevailing view was that no further study by the Secretariat was needed, since the fundamental issues were well known and it was clear that many aspects of battle-of-forms and adhesion contracts would need to be left to applicable national laws for reasons involving, for example, consumer protection and other public-policy considerations. After discussion, the Working Group decided that the issue should be dealt with as the first substantive item on its agenda, at the beginning of its next session.

IV. FUTURE WORK

156. The Working Group recalled that it had been requested by the Commission to examine the desirability and feasibility of preparing uniform rules on issues of digital signatures and certification authorities. At the close of its session, the Working Group felt that its report to the Commission should indicate that it had reached consensus as to the importance of, and the need for, working towards harmonization of law in that area. While it had not made a firm decision as to the form and content of such work, it had come to the preliminary conclusion that it was feasible to undertake the preparation of draft uniform rules on issues of digital signatures.

157. In the context of the discussion of future work, it was recalled that, alongside digital signatures and certification authorities, future work in the area of electronic commerce might also

---

2/ Ibid., Fifty-first Session, Supplement No. 17 (A/51/17), para. 222.

need to address: issues of technical alternatives to public-key cryptography; general issues of functions performed by third-party service providers; and electronic contracting (see A/51/17, paras. 219-221).